

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-149023

(43) 公開日 平成9年(1997)6月6日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/16			H 0 4 L 9/00	6 4 3
G 0 9 C 1/00	6 3 0	7259-5 J	G 0 9 C 1/00	6 3 0 Z
	6 6 0	7259-5 J		6 6 0 E

審査請求 未請求 請求項の数 5 O L (全 10 頁)

(21) 出願番号 特願平7-305435

(22) 出願日 平成7年(1995)11月24日

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 馬場 信行

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

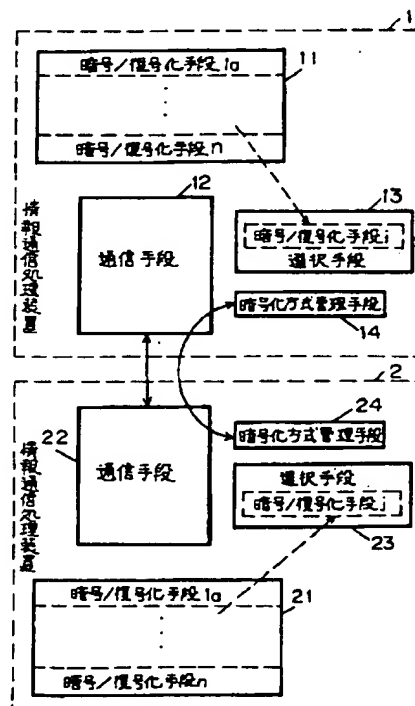
(74) 代理人 弁理士 滝本 智之 (外1名)

(54) 【発明の名称】 情報通信処理装置および情報通信処理方法

(57) 【要約】

【課題】 解読が困難なことにより機密が漏洩する可能性が極めて小さい情報通信処理装置および情報通信処理方法を提供することを目的とする。

【解決手段】 複数の暗号／復号化手段をテーブル化した暗号化方式テーブル11、21と、暗号化方式テーブル11、21から所定の規則によって1つの暗号／復号化手段を選択する選択手段13、23と、選択された暗号／復号化手段の暗号化方式テーブル11、21のオフセット値を相手側へ通知する暗号化方式管理手段14、24とを有することにより、機密が漏洩する可能性が極めて小さい情報通信処理装置および情報通信処理方法が得られる。



【特許請求の範囲】

【請求項1】複数の暗号／復号化手段をテーブル化した暗号化方式テーブルと、前記暗号化方式テーブルから所定の規則によって1つの暗号／復号化手段を選択する選択手段と、前記選択された暗号／復号化手段の前記暗号化方式テーブルのオフセット値を相手側へ通知する暗号化方式管理手段とを有する情報通信処理装置。

【請求項2】前記暗号化方式管理手段は、自己側と相手側とで異なる前記オフセット値を保持する請求項1記載の情報通信処理装置。

【請求項3】前記暗号化方式管理手段は、定められた時間間隔で前記オフセット値を変更して相手側へ通知する請求項1記載の情報通信処理装置。

【請求項4】前記暗号化方式管理手段は、定められた時間間隔で、前記暗号化方式テーブルを変更し、前記変更された暗号化方式テーブルのオフセット値を選択し、前記変更された暗号化方式テーブルおよび前記選択されたオフセット値を相手側へ通知する請求項1記載の情報通信処理装置。

【請求項5】複数の暗号化方式テーブルから所定の規則によって1つの暗号／復号化手段を選択する選択ステップと、前記選択された暗号／復号化手段の前記暗号化方式テーブルのオフセット値を相手側へ通知する暗号化方式管理ステップとを有する情報通信処理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、クレジット番号や機密文書等の文字データや画像／音声データを交換する情報通信処理装置および情報通信処理方法に関する。

【0002】

【従来の技術】近年、社会機構が複雑になるに伴い、機密文書等の漏洩防止の要請が高まりつつある。ところで、従来の情報通信処理装置では、扱うデータを暗号化しなかったり、単数もしくは複数の固定の暗号化方式で暗号化していた。また、同一のネットワーク内では同じ暗号化方式を利用する場合が多い。

【0003】

【発明が解決しようとする課題】しかしながら、上記の従来の情報通信処理装置では、機密漏洩防止を防止するのに十分な暗号化方式が使用されておらず、一部又はすべてのデジタルデータや音声データ、画像データが漏洩する可能性が大きいという問題点を有していた。

【0004】この情報通信処理装置においては、解読困難で機密漏洩の可能性が少ないことが要求されている。

【0005】本発明は、解読が困難なことにより機密が漏洩する可能性が極めて小さい情報通信処理装置および解読が困難なことにより機密が漏洩する可能性が極めて小さい情報通信処理方法を提供することを目的とする。

【0006】

【課題を解決するための手段】この目的を達成するため

に本発明は、複数の暗号／復号化手段をテーブル化した暗号化方式テーブルと、暗号化方式テーブルから所定の規則によって1つの暗号／復号化手段を選択する選択手段と、選択された暗号／復号化手段の暗号化方式テーブルのオフセット値を相手側へ通知する暗号化方式管理手段とを有するように構成したものである。

【0007】これにより、解読が困難なことにより機密が漏洩する可能性が極めて小さい情報通信処理装置が得られる。

10 【0008】

【発明の実施の形態】本発明の請求項1に記載の発明は、複数の暗号／復号化手段をテーブル化した暗号化方式テーブルと、暗号化方式テーブルから所定の規則によって1つの暗号／復号化手段を選択する選択手段と、選択された暗号／復号化手段の暗号化方式テーブルのオフセット値を相手側へ通知する暗号化方式管理手段とを有することとしたものであり、送信側で暗号化方式が任意に変更されるという作用を有する。

【0009】請求項2に記載の発明は、請求項1に記載の発明において、暗号化方式管理手段が自己側と相手側とで異なるオフセット値を保持することとしたものであり、接続された情報通信処理装置は互いに独立した暗号化方法で送信するという作用を有する。

【0010】請求項3に記載の発明は、請求項1に記載の発明において、暗号化方式管理手段が定められた時間間隔でオフセット値を変更して相手側へ通知することとしたものであり、定期的に暗号化方式が変更されるという作用を有する。

【0011】請求項4に記載の発明は、請求項1に記載の発明において、暗号化方式管理手段が、定められた時間間隔で、暗号化方式テーブルを変更し、変更された暗号化方式テーブルのオフセット値を選択し、変更された暗号化方式テーブルおよび選択されたオフセット値を相手側へ通知することとしたものであり、定められた時間間隔で暗号化方式テーブルのオフセット値のみならず暗号化方式テーブルをも変更されるという作用を有する。

【0012】請求項5に記載の発明は、複数の暗号化方式テーブルから所定の規則によって1つの暗号／復号化手段を選択する選択ステップと、選択された暗号／復号化手段の暗号化方式テーブルのオフセット値を相手側へ通知する暗号化方式管理ステップとを有することとしたものであり、送信側で暗号化方式を任意に変更されるという作用を有する。

【0013】以下、本発明の実施の形態について、図1から図9を用いて説明する。

（実施の形態1）図1は本発明の一実施の形態に係る情報通信処理装置を示すブロック図である。

【0014】図1において、1、2は機密文書等の文字データや画像／音声データを交換する情報通信処理装置、11、21は情報通信処理装置1、2の暗号／復号

3

化手段をテーブル化し、同一の内容を持つ暗号化方式テーブル、12、22は暗号化されたデータを送受信する通信手段、13、23は暗号／復号化手段を選択して格納する選択手段、14、24は選択された暗号／復号化手段を一方から他方へ、または相互に通知する暗号化方式管理手段である。暗号／復号化手段とは暗号化および復号化を行う手段であり、暗号化方式テーブル11、21のオフセット値で特定され、情報通信処理装置1、2のそれぞれを構成するノードのリンク数だけ存在する。オフセット値とは図1に示す1a、i、nといった番号値である。

【0015】以上のように構成された情報通信処理装置について、以下その動作を図2を用いて説明する。図2(a)は本実施の形態の動作を説明するための送信側のフローチャート、図2(b)は本実施の形態の動作を説明するための受信側のフローチャートである。まず図2(a)に示す送信側の情報通信処理装置の動作について説明する。ここでは情報通信処理装置1を送信側、情報通信処理装置2を受信側とする。送信側の選択手段13は、利用者の指定または利用者が定めた何らかの規則により、暗号化方式テーブル11から1つの暗号／復号化手段を選択する(S1、選択ステップ)。利用者が定めた何らかの規則とは、例えば1セッション間毎に暗号化方法を切り替えるといったような規則である。次に、暗号化方式管理手段14は、選択手段13で選択した暗号／復号化手段の暗号化方式テーブル11のオフセット値を記憶し、通信手段12を使って、接続する相手側(受信側)の情報通信処理装置2に通知する(S2、暗号化方式管理ステップ)。次に、暗号化方式管理手段14は、以後のデータ送受信に関し、選択した暗号／復号化手段を使ってデータの暗号化および復号化を行う(S3)。

【0016】次に、図2(b)に示す受信側の情報通信処理装置2の動作について説明する。暗号化方式管理手段24は、通信手段22によって受信した暗号化方式テーブル11のオフセット値を記憶し、選択手段23は暗号化方式テーブル21から対応する暗号／復号化手段を選択する(S11)。次に、暗号化方式管理手段24は、以後のデータ送受信に関し、選択した暗号／復号化手段を使ってデータの暗号化および復号化を行う(S12)。

【0017】このように本実施の形態1では、送信側で指定した暗号化方式に従って、送信側および受信側の情報通信処理装置1、2は情報の通信処理(暗号化および復号化の処理)を行う。すなわち、情報通信処理装置1、2は共に同じ暗号化方式で通信処理を行う。

【0018】以上のように本実施の形態1によれば、送信側で暗号化方式を任意に変更することができるので、情報の通信処理における機密保護レベルを向上させることが可能となる。

4

【0019】(実施の形態2)第2の実施の形態に係る情報通信処理装置の構成は図1と同じであるが、動作が異なる。

【0020】以上のように構成された第2の実施の形態に係る情報通信処理装置について、その動作を図3、図4を用いて説明する。図3は第2の実施の形態の動作を概略示す概略動作説明図であり、図4は第2の実施の形態の動作を説明するためのフローチャートである。

【0021】図3は情報通信処理装置1、2間でデータ通信を行った場合の時間的推移を示す。時間 $t_1 \sim t_2$ の送受信において、それぞれ異なる暗号化方式(1)、(2)によってデータ通信を行っている。

【0022】図4により、第2の実施の形態の動作を詳細に説明する。まず選択手段13、23は、利用者または利用者が定めた何らかの規則により、暗号化方式テーブル11、21から1つの暗号／復号化手段を選択する(S21)。次に、暗号化方式管理手段14、24は、選択手段13、23で選択した暗号／復号化手段の暗号化方式テーブル11、21のオフセット値を記憶し、通信手段12、22を使って、接続する相手側の情報通信処理装置1、2に通知する(S22)。暗号化方式管理手段14、24は、相手側情報通信処理装置1、2への以後のデータ送信に関し、選択した暗号／復号化手段を使ってデータの暗号化および復号化を行う(S23)。次に、暗号化方式管理手段14、24は、通信手段12、22によって相手側装置1、2より受信した暗号化方式テーブル21、11のオフセット値を記憶し、選択手段13、23は暗号化方式テーブル11、21から対応する暗号／復号化手段を選択する(S24)。暗号化方式管理手段14、24は、相手側情報通信処理装置1、2からの以後のデータ受信に関し、選択した暗号／復号化手段を使ってデータの暗号化および復号化を行う(S25)。

【0023】以上のように第2の実施の形態によれば、接続された情報通信処理装置1、2は互いに独立した暗号化方法で送信することができるので、互いに送信する暗号化方法を異なるものとしてことができ、暗号解読を一層困難なものとしてことができ、機密保護レベルを一層向上させることが可能となる。

【0024】(実施の形態3)第3の実施の形態に係る情報通信処理装置の構成は図1と同じであるが、動作が異なる。

【0025】以下、その動作について図5、図6、図7を用いて説明する。図5は第3の実施の形態の動作を概略示す概略動作説明図であり、図6、図7は第3の実施の形態の動作を送信側、受信側について説明するためのフローチャートである。

【0026】図5は情報通信処理装置1、2間でデータ通信を行った場合の時間的推移を示す。時間 $t_1 \sim t_2$ 、 $t_2 \sim t_3$ 、 $t_3 \sim t_4$ において、それぞれ異なる

暗号化方式(1)、(2)、(3)によってデータ通信を行っている。

【0027】図6により、第3の実施の形態の動作を送信側について詳細に説明する。図6は接続後の送信側情報通信処理装置における通信処理動作を示し、また、ここでは情報通信処理装置1を送信側、情報通信処理装置2を受信側とする。まず判別手段としての暗号化方式管理手段14は、あらかじめ利用者により指定された暗号/復号化手段の暗号化方式テーブル11のオフセット値を記憶し、通信手段12を使って接続する相手側(受信側)情報通信処理装置2に通知する(S32)。暗号化方式管理手段14は、相手側情報通信処理装置2との以後のデータ送受信に関し、指定した暗号/復号化手段を使ってデータの暗号化および復号化を行う(S33)。

【0028】図7により、第3の実施の形態の動作を受信側について詳細に説明する。図7は接続後の受信側情報通信処理装置2における通信処理動作を示す。まず暗号化方式管理手段24は通信手段22によって受信した暗号化方式テーブル11のオフセット値を記憶し、選択手段23は暗号化方式テーブル21から対応する暗号/復号化手段を選択する(S41)。暗号化方式管理手段24は、相手側情報通信処理装置1との以後のデータ送受信に関し、暗号化方式テーブル21上の選択された暗号/復号化手段(すなわち暗号化方式テーブル11上の指定された暗号/復号化手段)を使ってデータの暗号化および復号化を行う(S42)。

【0029】以上のように第3の実施の形態によれば、あらかじめ利用者により指定された暗号/符号化手段切替のタイミングで暗号/復号化手段を切り替える、すなわち定められた時間間隔でオフセット値を変更することにより、暗号解読を益々困難なものとする事ができるので、機密保護レベルを益々向上させることが可能となる。

【0030】(実施の形態4)第4の実施の形態に係る情報通信処理装置の構成は図1と同じであるが、動作が異なる。

【0031】以下、その動作について図8、図9を用いて説明する。図8、図9は第4の実施の形態の動作を送信側、受信側について説明するためのフローチャートである。

【0032】図8により、第4の実施の形態の動作を送信側について説明する。図8は接続後の送信側情報通信処理装置1における通信処理動作を示し、また、ここでは情報通信処理装置1を送信側、情報通信処理装置2を受信側とする。まず判別手段としての暗号化方式管理手

段14は、あらかじめ利用者により指定された暗号/符号化手段を切り替える、つまり暗号化方式を切り替えるタイミングか否かを判定する(S51)。切り替えるタイミングでない場合には待機状態となる。切り替えるタイミングの場合には、暗号化方式管理手段14は、あらかじめ利用者により指定された暗号化方式テーブル(変更された新たな暗号化方式テーブル)を記憶し、さらに、選択された暗号/復号化手段の上記新たな暗号化方式テーブルのオフセット値を記憶し、指定された新たな暗号化方式テーブルおよび新たな暗号化方式テーブル上の選択されたオフセット値を通信手段12を使って接続する相手側(受信側)情報通信処理装置2に通知する(S52)。暗号化方式管理手段14は、相手側情報通信処理装置2との以後のデータ送受信に関し、指定された暗号化方式テーブル上の選択された暗号/復号化手段を使ってデータの暗号化および復号化を行う(S53)。

【0033】図9により、第4の実施の形態の動作を受信側について説明する。図9は接続後の受信側情報通信処理装置2における通信処理動作を示す。まず暗号化方式管理手段24は通信手段22によって受信した上記新たな暗号化方式テーブルを記憶する(S61)。次に、暗号化方式管理手段24は通信手段22によって受信した上記新たな暗号化方式テーブル上の選択されたオフセット値を記憶し、選択手段23は暗号化方式テーブル21から対応する暗号/復号化手段を選択する(S62)。暗号化方式管理手段24は、相手側情報通信処理装置1との以後のデータ送受信に関し、指定された新たな暗号化方式テーブル上の選択された暗号/復号化手段を使ってデータの暗号化および復号化を行う(S63)。

【0034】以上のように第4の実施の形態によれば、あらかじめ利用者により指定された暗号/符号化手段切替のタイミングで暗号/復号化手段のみならず暗号化方式テーブルをも切り替える、すなわち定められた時間間隔で暗号化方式テーブルのオフセット値のみならず暗号化方式テーブルをも変更することにより、暗号解読を不可能なものとして万全の機密保護を図ることが可能となる。

【0035】

【発明の効果】以上のように本発明の情報通信処理装置によれば、送信側で暗号化方式を任意に変更することができるので、情報の通信処理における機密保護レベルを向上させることが可能な情報通信処理装置を実現することができるという有利な効果が得られる。また、接続された情報通信処理装置は互いに独立した暗号化方法で送信することができるので、互いに送信する暗号化方法を異なるものとする事ができ、暗号解読を一層困難なものとする事ができ、機密保護レベルを一層向上させることが可能な情報通信処理装置を実現することができるという有利な効果が得られる。さらに、定期的に暗号化

方式を変更することができるので、暗号解読を益々困難なものとし、機密保護レベルを益々向上させることが可能な情報通信処理装置を実現することができるという有利な効果が得られる。さらに、定められた時間間隔で暗号化方式テーブルのオフセット値のみならず暗号化方式テーブルをも変更することができ、暗号解読を不可能なものとして万全の機密保護を図ることが可能な情報通信処理装置を実現することができるという有利な効果が得られる。

【0036】本発明の情報通信処理方法によれば、送信側で暗号化方式を任意に変更することができるので、情報の通信処理における機密保護レベルを向上させることが可能な情報通信処理方法を実現することができるという有利な効果が得られる。

【図面の簡単な説明】

【図1】本発明の一実施の形態に係る情報通信処理装置を示すブロック図

【図2】(a) 本実施の形態の動作を説明するための送信側のフローチャート

(b) 本実施の形態の動作を説明するための受信側のフ

10

20

【図3】第2の実施の形態の動作を概略示す概略動作説明図

【図4】第2の実施の形態の動作を説明するためのフローチャート

【図5】第3の実施の形態の動作を概略示す概略動作説明図

【図6】第3の実施の形態の動作を送信側について説明するためのフローチャート

【図7】第3の実施の形態の動作を受信側について説明するためのフローチャート

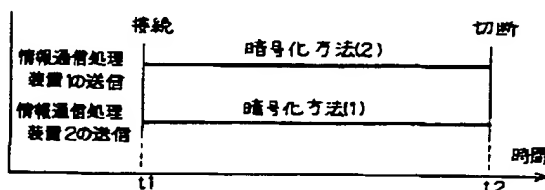
【図8】第4の実施の形態の動作を送信側について説明するためのフローチャート

【図9】第4の実施の形態の動作を受信側について説明するためのフローチャート

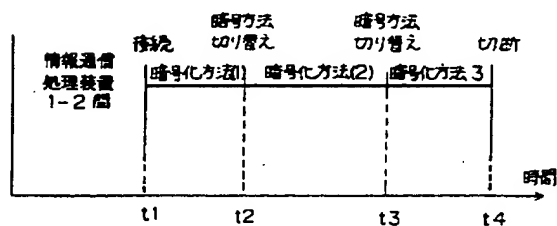
【符号の説明】

- 1、2 情報通信処理装置
- 11、21 暗号化方式テーブル
- 12、22 通信手段
- 13、23 選択手段
- 14、24 暗号化方式管理手段

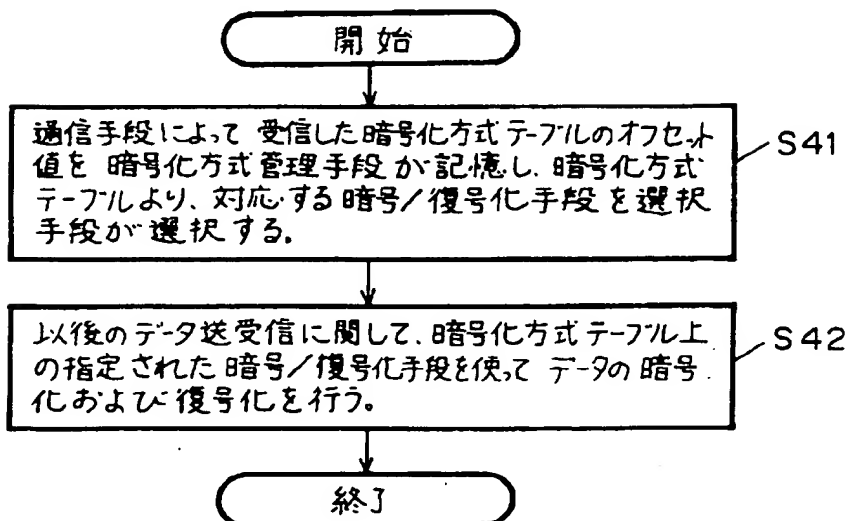
【図3】



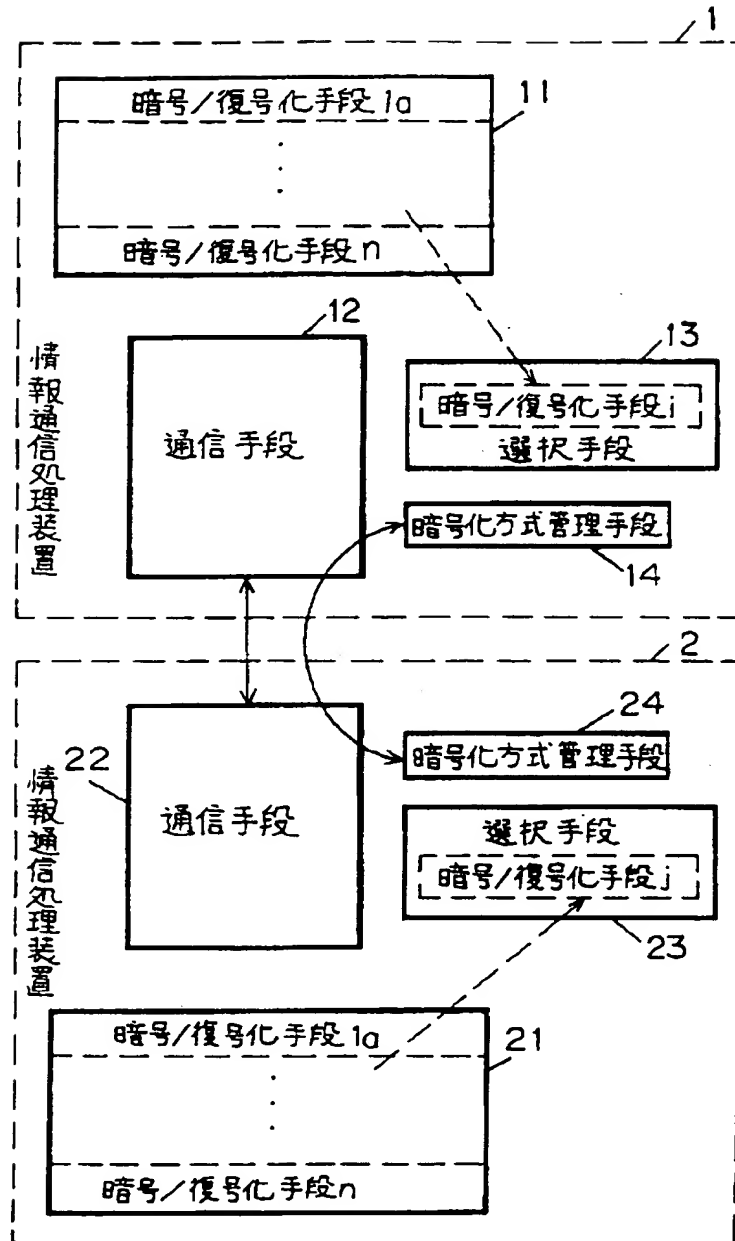
【図5】



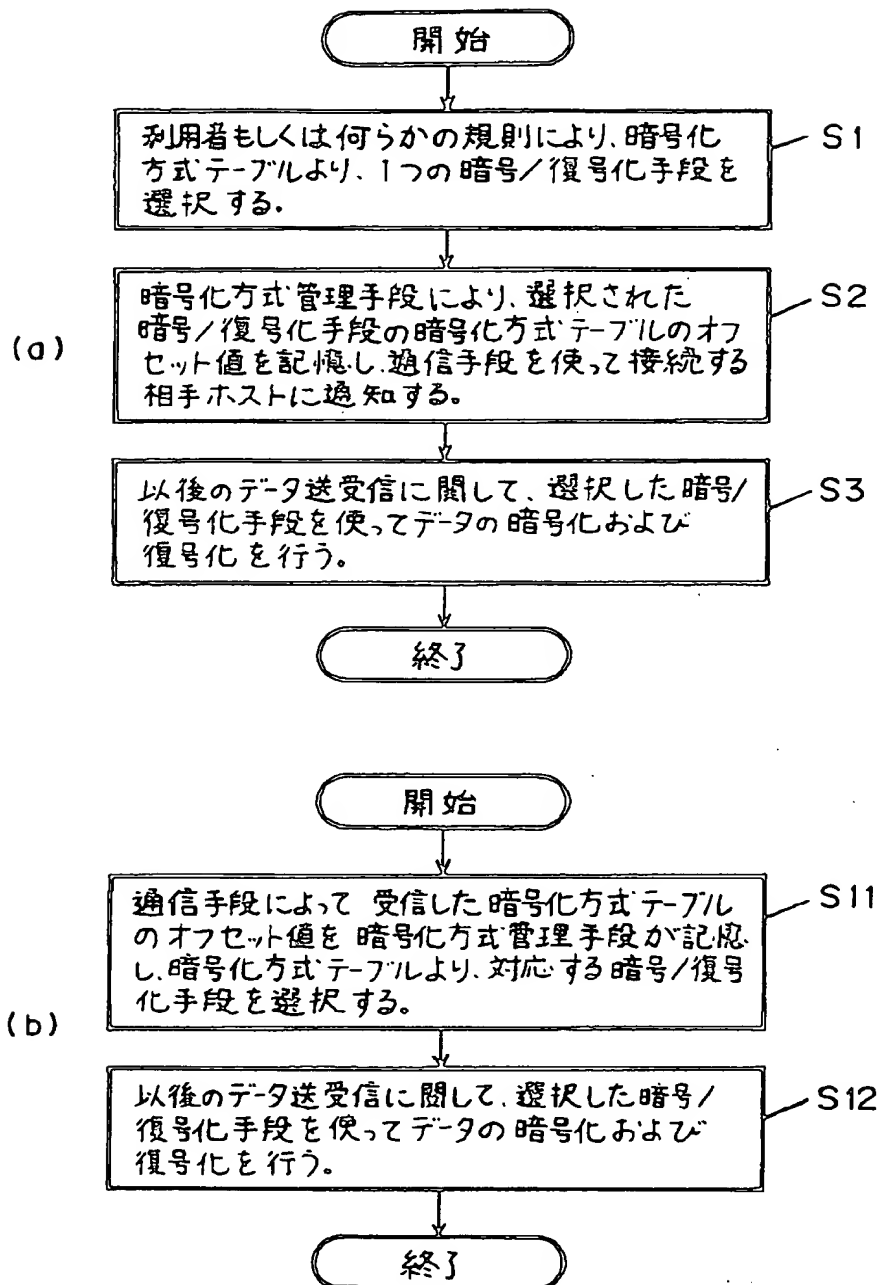
【図7】



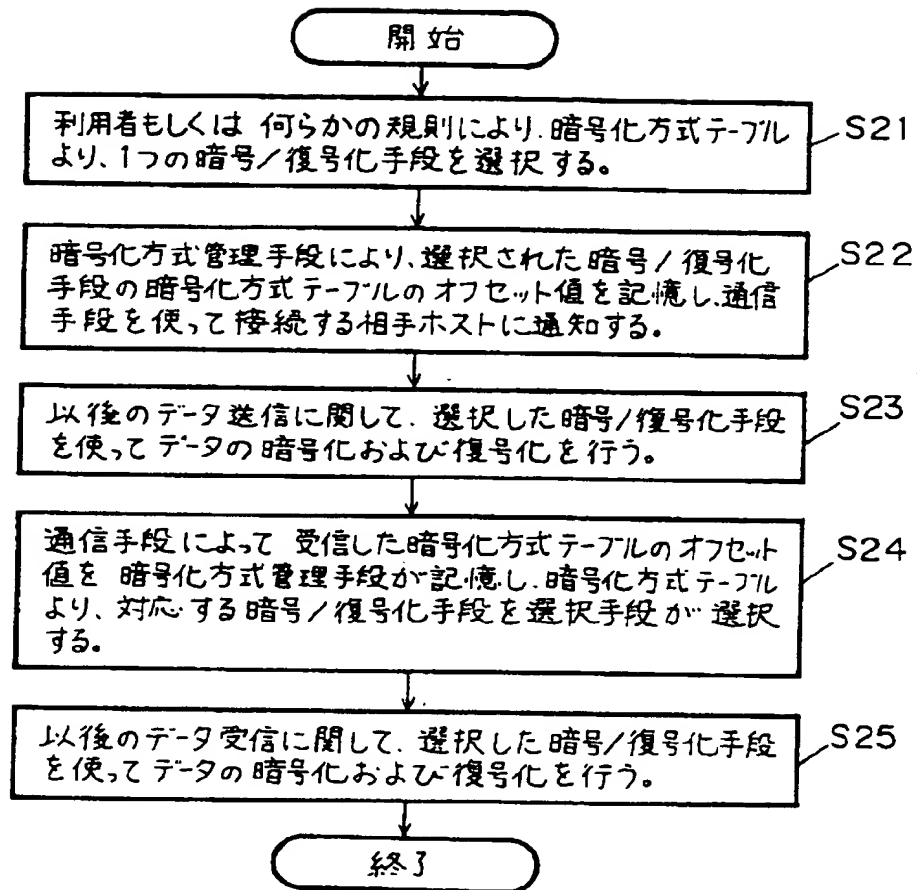
【図1】



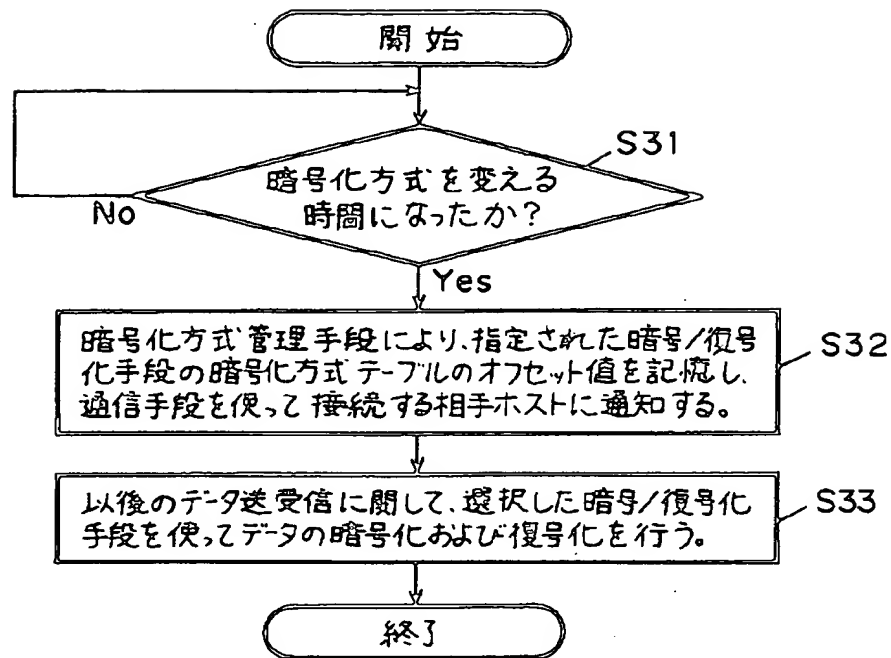
【図2】



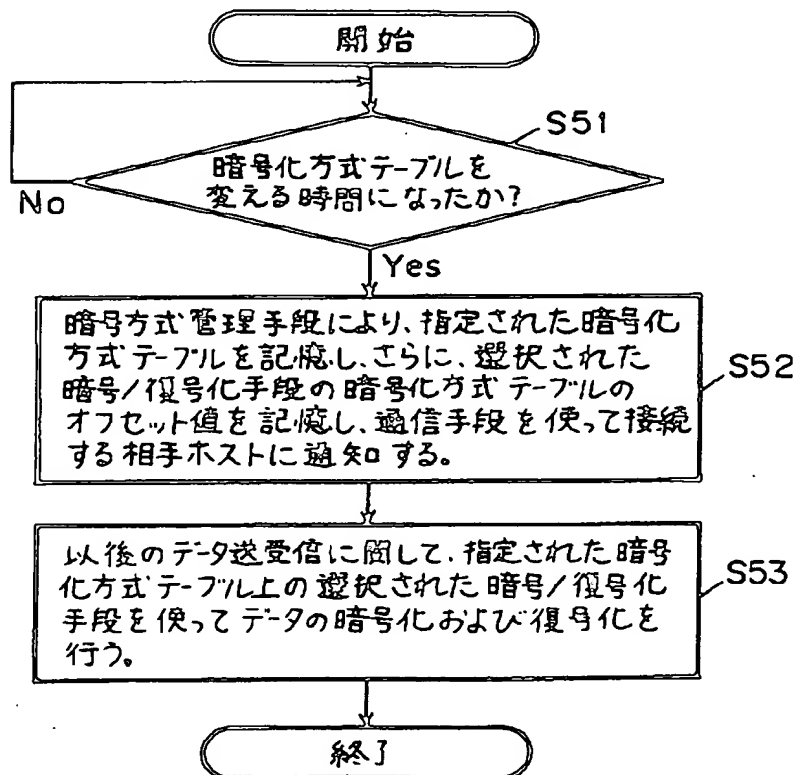
【図4】



【図 6】



【図 8】



【図9】

